Large Scale Sustainable Wireless Sensor Network: Algorithms and Protocols

Ph. D Synopsis

By

Deepak Vats

Registration No. 11 - PhD - 117

Under the supervision of

Dr. Devendra Prasad

Professor

M.M. Engineering College, Mullana, (Ambala)

DEPARTMENT OF INFORMATION TECHNOLOGY

M. M. Engineering College, Mullana, Ambala

Maharishi Markandeshwar University, Mullana

July 2013

Contents

1. Introduction

    1.1 Characteristics of Wireless Sensor Networks

    1.2 Constraints in Wireless Sensor Networks

    1.3 Applications of Wireless Sensor Network

2. Literature Review

    2.1 Energy Efficient Routing Protocols in WSNs

    2.2 Fault Tolerant Schemes in WSNs

    2.3 Secure Routing

3. Challenges

4. Objectives

Large Scale Sustainable Wireless Sensor Network: Algorithms and Protocols

Ph. D Synopsis

1. Introduction

A Wireless Sensor Network (WSN) is consisting of spatially distributed autonomous devices using sensors which enable pervasive, ubiquitous, and seamless communication with the physical world [1]. A few common applications are military, security, habitat monitoring, industrial automation, and agriculture, environmental observation and forecasting. It contains hundreds or thousands of sensor nodes (SNs)/Processing Element (PE) that have the ability to communicate either among each other or directly to the Base Station (BS). A BS is a fixed PE or a mobile PE that is capable of connecting the sensor network to an existing communications infrastructure or to the Internet. However, due to limited computing and storage resources, the sensors are not equipped with an enriched operating system that can provide energy efficient resource management thus; the application developers are responsible to incorporate energy efficient communication and routing strategies [2]. Although WSNs are similar to traditional mobile ad hoc networks (MANETs), there exist some fundamental differences between them. As WSNs need to work unattended and prone to failures, the processing in WSNs is data centric and WSNs use a broadcast communication scheme. In recognition to all differences between WSNs and other wireless networks, researchers are motivated to develop different solutions.

1.1 Characteristics of Wireless Sensor Networks

WSNs are an emerging technology currently being deployed in seismic monitoring, wild life studies, manufacturing and performance monitoring. In such scenarios the SNs are densely deployed in a predetermined geographical area to self-organize into ad hoc wireless networks to gather and aggregate data. Such networks typically contain a large number of the densely deployed SNs which function as a wireless peer-to-peer network. They use multi-hop and cluster based routing algorithms.

The ad hoc nature of WSNs poses unique challenges regarding their security and reliability. The limited memory, power, processing abilities and low coverage of the SNs make them vulnerable to intrusion, interception, modification and fabrication and traditional security techniques cannot ensure confidentiality, integrity, reliability and availability. Therefore new

security measures are needed to address the specific security challenges of WSNs.

1.2 Constraints in Wireless Sensor Networks

Constraints in WSNs are unique compared to traditional networks making the implementation of existing security measures impractical. In broader terms, these constraints are the result of limitations regarding the SNs' memory, energy, transmitting and processing power as well as due to the ad hoc and wireless channel. These constraints, which make the design of security procedures more complicated, have been categorized into node constraints and network constraints and are discussed in the following section.

Security solutions require a high computation, memory, storage and energy resource which creates an additional challenge when working with tiny SNs. Table 1.1 lists the specifications of three different types of SNs used in WSNs: Crossbow's MICA2, CSIRO's FLECK and Crossbow's Imote.

Table 1.1 Specifications of three different types of sensors

Specifications	**Crossbow's (MICA2)**	**CSIRO's (FLECK)**	**(Imote)**
Processor	8MHz, Atmel ATMega128L	4MHz, Atmel ATMega128L	13-416 MHz, Intel PXA271 XScale
Memory	128KB Program Flash and 4KB RAM	512KB Program Flash	256KB SRAM, 32MB SDRAM
External storage	512KB Serial Flash	1 MB (Fleck3)	32MB Flash
Default power	2.7v – 3.3v 2xAA	1.3v – 5.3v includes	3.2v – 4.5v 3xAAA
Sleep mode	<15 microA	230 microA	390 microA
Radio	916MHz	433 MHz	2400 MHz
LEDS	3 LED indicators	3 LED	
Size	58 x 38 mm	60 x 60mm	36 x 48 x 9 mm
Range	300m	500m	30m (line of sight with integrated
OS	TinyOS	TinyOS	TinyOS

- **Memory:** Memory in a sensor node usually includes flash memory and RAM. Flash memory is used for storing downloaded application code and RAM is used for storing application programs, sensor data and intermediate computations. There is usually not enough space to run complicated algorithms after loading OS and application code. In the SmartDust project, for example, TinyOS consumes about 3500 bytes of instruction memory, leaving only 4500 bytes for security and applications. This makes it impractical to use the majority of current security algorithms. With an Intel Mote, the situation is slightly improved, but still far from meeting the requirements of many algorithms.

- **Energy:** Energy consumption in SNs can be categorized into three parts: Energy for the sensor transducer, Energy for communication among SNs and Energy for microprocessor computation. It has been found that each bit transmitted in WSNs consumes about as much power as executing 800–1000 instructions. Thus, communication is more costly than computation in WSNs. Any message expansion caused by security mechanisms comes at a significant cost. Further, higher security levels in WSNs usually correspond to more energy consumption for cryptographic functions. Thus, WSNs can be divided into different security levels, depending on energy cost.
- **Computation:** The embedded processors in SNs in wireless sensor network are generally not as powerful as those in SNs of a wired or ad hoc network. As such, complex cryptographic algorithms cannot be used in WSNs.

WSNs inherit all the constraints of mobile ad hoc networks such as unreliable network communication, collision and lack of physical infrastructure.

- **Communication:** Wireless communication is inherently unreliable and can cause packets to be damaged or dropped. This unreliability in communication poses additional threats to the SNs if dropped packets are taken over by adversaries.
- **Collisions and latency:** In sensitive applications concentration of SNs are very high. This causes collision and latency in packets. However, unlike in traditional networks, the energy limitation of SNs makes it impracticable to resend packets in case of collision.

In many cases WSNs are installed in public and potentially hostile environments which makes some of their components damaged and highly vulnerable to capture. To physically secure SNs with tamper proof material increases the cost.

- **Unattended Nature:** In an application where WSN are deployed in hostile environment and left unattended allows adversaries greater access and freedom to physically tamper with the SNs. Extreme weather conditions and natural disasters such as storms, floods, earth quakes and fires can also affect their functioning.
- **Remotely managed:** In hostile environment where WSNs are remotely managed, it is quite difficult to detect physical tampering with the WSNs; other issues such as replacing the batteries and redeploying cryptographic keys are also impracticable.

1.3 Applications of Wireless Sensor Network

Sensor networks can be deployed in a wide variety of applications. One of the main classification criteria is whether the SNs are mobile or immobile [3]. The data collection might

be either continuous or periodic; the latter can lead to busty traffic patterns. Naturally, every application requires a specific set of sensor types. Some of the most popular sensor types are: light, sound, magnetic field, accelerator, temperature, humidity, chemical composition such as soil makeup, mechanical stress levels on an object and many others. Some of the primary application domains for sensor networks are the following:

- **Environmental:** Environmental sensors can be used to detect and track natural disasters such as forest fires or floods. They can also be used to track the movement of birds and other animals.
- **Military.** The sensor networks will be an integral part of the future systems (command, control, communications, computing, intelligence, surveillance, reconnaissance, and targeting). They can, for instance, be used to track the movement of the enemy in the battlefield. The main advantage of WSNs is that they can be deployed and operated remotely, without putting human lives at risk. Naturally, military deployments bring their own challenges of security and confidentiality.
- **Health.** Sensors can be also used to track and monitor the drug doses prescribed to patients and prevent situations where the drugs are administered to the wrong patient. Sensors can be deployed for telemonitoring of patients, a promising new direction for at-home monitoring and care for the elderly.
- **Home.** The various home appliances can be sensor enabled and interconnected with each other and a central control system of the home. These sensor-enabled sensor homes might not only offer additional conveniences, but will also be safer and more energy efficient.
- **Solar Energy.** The material of the photovoltaic cell in the solar panel is doped in such a way that when the solar radiation is absorbed by the cell, the solar energy from the sun would be harvested and converted into electric energy leading to Sustainable Wireless Sensor Networks [4].

2. Literature Survey

One of the most active research areas in wireless sensor networks is the coverage. Coverage is usually interpreted as how well a sensor network will monitor a field of interest. Coverage can be measured in different ways depending on the applications. In addition to coverage it is important for a sensor network to maintain connectivity. Connectivity can be defined as the ability of the sensor nodes to reach the data sink. If there is no available route from a sensor node to the data sink then the data collected by that node cannot be processed. Each node has a communication range which defines the area in which another node can be located in order to receive data. This is separate from the sensing range which defines the area a node can observe. The two ranges may be equal but are often different.

There are several factors that must be considered during the deployment of sensor networks. Many of these will be dependent upon the particular application that is being addressed. The capabilities of the sensor nodes that are being used must also be considered. Most researchers focus on a single deployment model but there are papers that attempt to develop a more general algorithm that can be used in many types of deployment.

Most of the times sensor nodes are deployed in hostile and unstable environment conditions, so changes in the environment usually damage the sensor nodes deployed in certain regions which lead broken connectivity hence partitioning the network into small networks. Sensor Nodes in these partitioned networks still capable of sensing the events occurring in their sensing range but are not able to disseminate data to the Base Station, which makes the whole infrastructure useless.

2.1 Energy Efficient Routing Protocols in WSNs

Routing protocols have a large scope of research work when implemented in WSNs, because the functioning of these protocols depends upon the type of network structure designed for the application or the network operations carried out using these protocols for a specific application model.

a). Flat Routing Protocols in WSNs

In flat networks, each SN typically plays the same role and SNs collaborate together to perform the sensing task. Due to the large number of such SNs, it is not feasible to assign a global identifier to each SN. This consideration has led to data centric routing, where the BS sends queries to certain regions and waits for data from the sensors located in the selected regions. Since data is being requested through queries, attribute-based naming is necessary to specify the properties of data. Early works on data centric routing, viz., Sensor Protocols for Information via Negotiation (SPIN) [5] and Directed Diffusion [6] has minimizes the energy issue through data

negotiation and elimination of redundant data. Rumor routing [7] is a variation of directed diffusion and is mainly intended for applications where the geographic routing is not feasible.

b). Hierarchical Routing Protocols in WSNs

A heterogeneous SN is more expensive and is capable to provide data filtering, fusion and transport. It may posses one or more type of heterogeneous SNs, e.g., enhanced energy capacity or communication capability. They may be line powered, or their batteries may be replaced easily. Compared with the normal SNs, they may be configured with more powerful microprocessor and more memory. They may communicate with the BS via high bandwidth, long-distance network, such as Ethernet. The presence of heterogeneous SNs in a WSN can increase network reliability and lifetime. The main basic and important deployment problem is to decide how many and where heterogeneous SNs should be deployed in the network.

The heterogeneous resources are basically divided into three categories: computational heterogeneity, link heterogeneity and energy heterogeneity [8].

Computational heterogeneity signifies that the heterogeneous SN has a more powerful microprocessor or microcontroller and more storage memory than the normal SN. The SNs with more powerful computational resources can provide complex data processing and longer-term storage.

Link heterogeneity means that the heterogeneous SN has high-bandwidth and long haul network transceiver (Ethernet or 802.11) network, than the normal SN. Link heterogeneity can provide more reliable data transmission. Therefore, the reliability of the data transmission will increase by link heterogeneity.

Energy heterogeneity means that the heterogeneous SN is line powered, or its battery is replaceable. Among above three categories of resource heterogeneity, the energy heterogeneity is most important because both computational heterogeneity and link heterogeneity will consume more battery energy resource. If there is no energy heterogeneity, computational heterogeneity and link heterogeneity will bring negative impact to the WSN.

Hierarchical or cluster-based routing, are well known techniques with special advantages related to scalability and efficient communication. The concept of hierarchical routing is utilized to perform energy-efficient routing in WSNs. In a hierarchical architecture, higher energy SNs can be used to process and send the information while low energy SNs can be used to perform the sensing in the proximity of the target. Some of routing protocols in this group are: Low-Energy Adaptive Clustering Hierarchy (LEACH) [3], Power-Efficient Gathering in Sensor Information System (PEGASIS) [9], Threshold-Sensitive Energy Efficient TEEN [10] and Adaptive Threshold-Sensitive Energy Efficient (APTEEN) [11].

In LEACH cluster is formed on the basis of received signal strength and local CH is selected to route the data to the BS. The CH is elected randomly and rotated among the SNs in the cluster. The cluster head communicates directly with the BS and neighboring CH in the network.

In [12], authors introduce CH Election mechanism using Fuzzy (CHEF) logic. They apply the fuzzy if-then rule to the CH election mechanism. By using fuzzy logic, the computational overhead is reduced and the network lifetime is extended. In addition, the operation of this mechanism is localized. The BS does not collect and elect CHs. The SNs only elect CHs among themselves using the fuzzy logic. The routing protocol [13] based on dynamic clustering protocol which grants a large lifetime for the network. The key idea of this protocol is to reduce transmission in intra-clusters when the objective is to collect the maximum or minimum data values in a region (like temperature, humidity, etc.).

The authors have presented a novel CH election problem in [14], specifically designed for applications where the maintenance of full network coverage is the main requirement. This approach is based on a set of coverage-aware cost metrics that favor SNs deployed in densely populated network areas as better candidates for CH SNs, active SNs and routers. Compared with traditional energy-based selection methods, the coverage-aware selection of CH SNs increases the network lifetime depending on the application scenario.

In [15], authors have presented an important corona model to maximize the network lifetime by using adjustable transmission range. In this model the maximum transmission range of sensors is divided into several levels. The sensors SNs belong to the same corona have the same range of transmission, whereas different coronas have different transmission ranges. The authors concluded that transmission ranges to all coronas is the effective approach to extend the network lifetime.

In [16], authors have proposed a non-uniform SN distribution strategy to achieve the sub-balanced energy depletion. In this strategy if the number of SNs in coronas increases then the network can achieve sub-balanced energy depletion.

PEGASIS [10] discusses how to extend the lifetime of WSNs. It is a near optimal chain-based protocol, not a clustering scheme. In PEGASIS, each SN communicates only with an adjacent neighbor and takes turns transmitting to the BS. A number of issues are discussed, viz., reducing the amount of energy spent per processing round, minimizing overall distance between non-leader SNs of the system and minimizing the number of data transmission to the BS. However, in PEGASIS, SNs die in random locations since the CHs have been chosen without any concern on an overall lifetime of each SN.

To prolong the network lifetime by distributing energy consumption, HEED (Hybrid Energy-Efficient Distributed Clustering) [17] is a standalone distributed clustering approach in which each SN considers two factors: remaining energy and communication cost before making a decision to join one cluster or the other. In HEED, once selected a CH is maintained for a fixed number of iterations. This is in contrast to some other approaches where the CHs are newly selected in every step. This is to reduce the unnecessary high setup cost associated with the CH selection process.

2.2 Fault Tolerant Schemes in WSNs

SNs in WSNs are prone to failure due to energy depletion, hardware failure, communication link errors, malicious attack and so on. Unlike the cellular and ad hoc networks where energy has no limits in BS or batteries can be replaced as needed, SNs in WSNs have very limited energy and their batteries cannot usually be recharged or replaced due to hostile or hazardous environments. So, one important characteristic of WSNs is the stringent power management of the SNs. Two components of a SN, viz., sensing unit and wireless transceiver, usually directly interact with the environment which is subject to variety of physical, chemical and biological factors. It results in low reliability of performance of the SNs. Even if condition of the hardware is good, the communication between the SNs are affected by many factors, such as signal strength, antenna angle, obstacles, weather conditions, interference.

The services provided by a WSN to a large extent depend on fault tolerance, because it cannot be assumed that all sources of error can be eliminated, even through careful engineering. By considering service availability, we understand the probability with which a request will lead to a valid and useful response. The availability of WSN is defined as: $P(A)=\frac{MTTF}{MTTF+MTTR}$ where MTTF stands for Mean Time to Failure and MTTR stands for Mean Time to Repair [18].

By analyzing this equation we can conclude that systems that constantly fail and require long repair time will result in systems with very low availability. However, systems that have a high MTTF and can be quickly repaired are considered highly available systems.

Attacks on the availability of SNs are analyzed in [19]. These attacks directly influence the availability of services. Fault tolerant systems can overcome faults and system failures, therefore increasing the MTTF and system availability. Fault tolerance techniques especially crafted for WSNs have not been extensively studied so far. The most important one is replication, which is well suited for WSNs due to their inherent SN redundancy. Fault Tolerance has been discussed in detail in the literature on distributed systems [20]. Although WSNs have special characteristics

that distinguish them from traditional distributed systems, many of the existing techniques still apply.

To comprehend fault tolerance mechanisms, it is important to point out the difference between faults, errors and failures. Various definitions of these terms have been used [21]. This article refers to the definition given in [22]:

- A fault is any kind of defect that leads to an error.
- An error corresponds to an incorrect (undefined) system state. Such a state may lead to a failure.
- A failure is the (observable) manifestation of an error, which occurs when the system deviates from its specification and cannot deliver its intended functionality.

There are five levels of fault tolerance, viz., physical layer, hardware layer, system software layer, middleware layer and application layer [23]. Based on the study, we classify fault tolerance in WSNs into four levels from the system point of view. More specifically, fault tolerance in a WSN system may exist at hardware layer, software layer, network communication layer and application layer.

Faults at hardware layer can be caused by malfunction of any hardware component of a SN, such as memory, battery, microprocessor, sensing unit and network interface (wireless radio). There are three main reasons that cause hardware failure of SNs. The first is that WSNs are usually for commercial use and SNs are cost sensitive. Therefore, design of a SN will not always use the highest quality components. The second is that strict energy constraints which restrict long and reliable performance of SNs. In [24-25] due to stress from the environment and inadequate enclosures, the SNs were exposed to direct contact with water causing short circuits. The third is that WSNs are often deployed in harsh and hazardous environments which affect normal operation of SNs. The wireless radios of SNs are severely affected by these environment factors.

Software of a SN consists of two components: system software, such as operating system and middleware, such as communication, routing and aggregation. An important component of system software is to support distributed and simultaneous execution of localized algorithms. Software bugs are a common source of errors in WSNs. One promising method is through software diversity where each program is implemented in several different versions. Since it is difficult to provide fault tolerance in an economic way at hardware level of a SN, numerous fault-tolerant approaches are expected at the middleware level. The majority of current applications in WSNs are simple. To adapt the real-life applications, there is a need to develop much more complex middleware for WSNs.

Faults at network communication layer are the faults on wireless communication links. Assuming that there is no error on hardware, link faults in WSNs are usually related to surrounding environments. In addition, link faults can also be caused by radio interference of SNs. For example, SN ‘a’ cannot successfully receive a message from SN ‘b’ if SN ‘a’ is within interference range of other SNs that are transmitting messages at the same time. The standard way to enhance the performance of wireless communication is to use aggressive error correction schemes and retransmission. These two methods may cause further delay of operation. It should be pointed out that there is always a trade-off between fault tolerance and efficiency. In WSNs, communication links between SNs are highly volatile and are not always yield the same delivery rate of messages in field trials as in lab trials.

In [26], authors present an experimental study on fault tolerant routing for wireless sensor grid networks. A network may be separated into partitions owing to the broken radio links resulted from SN failures. Since the leveling algorithm works effectively for un-partitioned network, a combined technique with extended transmission range is investigated to resolve the network-partitioning problem. In [27], authors propose FTPASC (Fault Tolerant Power Aware protocol with Static Clustering), a static clustering based protocol, which engages high power SNs for power consuming tasks and as a result extends the network lifetime. In classical static clustering, when the CHs energy was depleted all the SNs of that cluster lose their communication with the BS and become essentially dead. In each cluster, FTPASC chooses the SN with maximum energy as the CH. Thus, not only there is always one CH for each cluster, but also the overhead of dynamic clustering is removed.

2.3 Secure Routing

The goal of networking is to provide an infrastructure for delivering data from a source node to a destination node. Routing protocols are the most critical component because they address the problem of how to find a path from the source to the destination and finally take charge of data delivery. In this way, the nodes in a network can collaborate with each other to fulfill various applications deployed in advance. If routing protocols fail under malicious attacks, the high layer applications also fail and the network is useless. Therefore, secure routing is very important to guarantee the network functionality in the face of malicious attacks.

To minimize energy consumption, routing techniques for WSNs employ well-known tactics, as well as those particular to WSNs. For example, in flat routing protocols such as directed diffusion [28], data aggregation and in-network processing are required to reduce the number of transmissions of redundant data. Clustering is a critical process to build up a hierarchical WSN in hierarchical routing protocols such as the low energy adaptive clustering hierarchy (LEACH) [29]. Sensor nodes in the local area cooperate to select a cluster head that may be more powerful

so that it can perform more complex operations such as data aggregation or long distance routing. In location-based routing protocols such as Geographical and Energy-Aware Routing (GEAR) [30], the location of a sensor node, which can be estimated by global positioning system (GPS) devices or GPS-free methods, is used as the routing metric. However, most routing protocols for WSNs do not consider security in their designs. Karlof and Wagner [31] pointed out that most routing protocols for WSNs are vulnerable to malicious attacks. Unencrypted packets that carry routing information can be easily subject to eavesdroppers so that attackers can discover the network topology. Attackers can inject false routing information to launch a Sybil attack [32] and redirect packets to change network topology. Both of the attacks can change the network traffic pattern so that some malicious nodes can receive most of the traffic before it arrives at the BS. In data aggregation, the aggregation node can be compromised so that the aggregated data is tampered with. A non-aggregation node also can report false data to the aggregation node to disrupt the final report. A location deterministic operation is vulnerable because it requires cooperation among several nodes and may not be successful if some of them are malicious. A malicious node intentionally may drop some of the passing traffic. Of course, it can drop all the packets to act like a black hole, but this is easy to detect. Selective forwarding is more difficult to detect. A malicious node may drop the packets from some selected nodes and forward those from other nodes. A more subtle way is to drop packets intermittently so that it behaves like an unstable channel. Most routing protocols require that each sensor node periodically broadcast routing information to maintain the network topology. If the time synchronization in the maintenance operation is attacked [33, 34], the whole network fails. Though several proposals [35-37] tried to secure ad hoc routing protocols, they hardly can be applied in WSNs for three reasons. First, all proposals target ad hoc networks, which are different from WSNs in terms of resources and communication patterns. Second, those proposals are security extensions of existing ad hoc routing protocols such as dynamic source routing (DSR), ad hoc on-demand distance vector (AODV), or destination-sequenced distance vector (DSDV) [38], which are not suitable for WSNs. Third, those proposals require either asymmetric key cryptography or complicated symmetric key cryptography, which are expensive on sensor platforms.

There are several possible security countermeasures for securing routing protocols. Link-layer encryption and authentication by using a global key can protect WSNs against external attackers because they do not know the global key. However, this does not secure against node compromise because the global key can be exposed. A trustful BS can detect spoofed node identities if every node shares a unique key with it, which is studied in SPINS [39]. However, the centralized control can introduce too much communication or management overhead. To counter

selective forwarding by malicious nodes, multipath routing can be used to increase the probability of data delivery. To support topology maintenance, authentication is required to protect broadcast of routing information in a local area. Though these methods effectively can prevent external attackers from spoofing, modifying, and replaying information and reduce the impact of selective forwarding, they cannot protect the network from internal malicious nodes efficiently.

In the INtrusion-tolerant routing protocol for wireless SEnsor NetworkS (INSENS) [40], the authenticated routing information can be collected by the BS so that it can calculate the routing table for every sensor node. The broadcast infor- To prevent DoS attacks, individual nodes are not allowed to broadcast information to the entire network. To increase the tolerance to node compromise, redundant multipath routing is used so that traffic can survive even if some paths are compromised. However, INSENS assumes an application scenario where communications can happen only between sensor nodes and the BS. It does not support in-network processing. Pietro *et al*. proposed an extension of logical key hierarchy for WSN (LKHW) [41] to protect the directed diffusion protocol. An LKH is a key tree structure with source nodes as leafs and a sink node as the root. Each leaf node holds keys along the path from it to the root node. In LKHW, an LKH is established before data are fused. Then the LKH is used to provide encryption and authentication for data fusion. A hierarchical network is constructed with cluster heads and cluster member nodes. Messages from sensor nodes are routed by cluster heads. To protect data, a preloaded symmetric key is shared between all cluster heads and the base BS.

3. Challenges

- One of the most active research areas in wireless sensor networks is the coverage. Coverage is usually interpreted as how well a sensor network will monitor a field of interest. Coverage can be measured in different ways depending on the applications. In addition to coverage it is important for a sensor network to maintain connectivity. Connectivity can be defined as the ability of the sensor nodes to reach the data sink. If there is no available route from a sensor node to the data sink then the data collected by that node cannot be processed. Each node has a communication range which defines the area in which another node can be located in order to receive data. This is separate from the sensing range which defines the area a node can observe. The two ranges may be equal but are often different.
- A key challenge in Wireless Sensor Networks (WSNs) is ensuring the sustainability of the system at the required performance level, in an autonomous manner. Sustainability is

a major concern in WSNs because of severe resource constraints deices in terms of energy, bandwidth and sensing capabilities are used in the system. Routing protocols for wireless sensor networks are responsible for maintaining the routes in the network and have to ensure reliable communication under these conditions. However, due to inherent resource and computing constraints, solutions dedicated to other networks (e.g. wired) are not well suited in WSNs. There is currently enormous research potential in the field of sustainable WSNs.

- For routing protocols, security considerations should be considered at the design stage. Considering specific application scenarios, the network administrator should analyze the possible black holes that may corrupt or disrupt the applications and deploy security countermeasure in advance. A general approach to protect routing protocols is to authenticate the routing information exchanged between nodes. This can effectively prevent an external attacker from injecting false routing information. However, authenticated routing metrics may not be correct in that an internal malicious node can claim false routing metrics without being detected because it has correct keys. Therefore, it is necessary for high layers to verify routing metrics. Some metrics such as residual energy are very difficult to verify because each node cannot know the energy consumption of other nodes. The metrics that have local similarity are easy to verify. For example, most geographical routing protocols have inherited immunity to false routing information because the nodes that are close to each other should have similar geographical distances to the sink. Considering the frequent node failure under malicious attacks, multipath routing is a promising approach to provide robust and secure data transmission services. However, the integration of security measures into routing protocols can introduce additional overhead. Strong security primitives can ensure a high level of security but may not be acceptable because of the resource constraints of WSNs. How to achieve a trade-off between security and routing overhead is still an open problem.

4. Objectives

The area of sustainable wireless sensor networks is very broad with many topics and open problems. With the widespread use of sustainable WSN deployments, the need for reliable security mechanisms will grow significantly. Existing solutions are not sufficient for many applications and new routing schemes need to be developed. The development of efficient routing protocols/algorithms is challenging because sensor nodes are prone to failures and the network topology changes frequently. Few of the following will be developed to obtain the

sustainability in large scale WSN.

- Energy Efficient routing Protocols/Algorithms will be proposed to overcome many of the shortcomings of existing Protocols/Algorithms.
- Fault Tolerance routing Protocols/Algorithms will be developed to make wireless sensor network self reconfigurable to maintain the connectivity of the network.
- Secure routing Protocols/Algorithms will be developed to support mobile sensor networks.
- For performance viewpoint, developed Protocols/Algorithms will be compared with some existing Protocols/Algorithms.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless Sensor Networks: A Survey", Computer Networks Journal, Elsevier Science, Vol. 38, No. 4, pp. 393–422, March 2002.

[2] J. A. Al-Karaki and A. E. Kamal, "Routing Techniques in Wireless Sensor Networks: A Survey", IEEE Wireless Communication, vol. 11, no. 6, Dec. 2004.

[3] Alan Mainwaring, Joseph Polastre, Robert Szewczyk, and David Culler. "Wireless Sensor Networks for Habitat Monitoring", In First ACM International Workshop on Wireless Sensor Networks and Applications, Sept. 28, 2002.

[4] H. Zhang and J. C. Hou. "Maintaining Sensing Coverage and Connectivity in Large Sensor Networks", International Journal of Wireless Ad Hoc and Sensor Networks, vol. 1, pp 89-124, March 3, 2005.

[5] J. Tateson, C. Roadknight, A. Gonzalez, T. Khan, S. Fitz, I. Henning, N. Boyd, C. Vincent, "Real World Issues in Deploying a Wireless Sensor Network for Oceanography", In Proceedings of Workshop on Real-World WSNs, Stockholm, Sweden, 20-21 June 2005.

[6] C. Intanagonwiwat, R. Govindan, D. Estrin, "Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensors Networks", In Proceedings of 6th Annual International Conference on Mobile Computing and Networking, Boston, MA, USA, pp. 56-67, 6-11 August 2000.

[7] D. Braginsky, D. Estrin, "Rumor Routing Algorithm for Sensor Networks", In Proceedings of First ACM International Workshop on WSNs and Applications (WSNA), Atlanta, Georgia, USA, pp. 22-31, 28 September 2002.

[8] G. Amato, A. Caruso, S. Chessa, "Application driven Energy Efficient Communication in WSNs", Elsevier, Computer Communication, Vol. 32, No. 5, pp. 896-906, March 2009.

[9] S. Lindsey, C.S. Raghavendra, "PEGASIS: Power-Efficient Gathering in Sensor Information Systems", SIGMOD record, Vol. 32, No. 4, pp. 66-71, December 2003.

[10] A. Manjeshwar, D.P. Agrawal, "TEEN: A Routing Protocol for Enhanced Efficiency in WSNs", In Proceedings of 15th International Parallel and Distributed Processing Symposium (IPDPS) Workshops, San Francisco, California, USA, pp 1964- 1975, 23-27 April 2001.

[11] A. Manjeshwar and D.P. Agrawal, "APTEEN: A Hybrid Protocol for Efficient Routing and Comprehensive Information Retrieval in WSNs", In Proceedings of International Parallel and Distributed Processing Symposium (IPDPS), Fort Lauderdale, FL, pp. 195-202, 15-19 April 2002.

[12] J.M. Kim, S.H. Park, Y.J. Han, T.M. Chung, "CHEF: CH Election Mechanism Using Fuzzy Logic In WSNs", In Proceedings of 10th International Conference on Advanced Communication Technology (ICACT), Phoenix Park, Korea, pp.654-659 Vol. 1, 17-20 February 2008.

[13] O. Zytoune, M. Aroussi, M. Rziza, D. Aboutajdine, "Stochastic Low Energy Adaptive Clustering Hierarchy", Journal of Computer Networks and Internet Research ICGST-CNIR, Vol. 8, No. 1, pp.47-51, 2008.

[14] S. Stanislava, W.B. Heinzelman, "CH Election Techniques for Coverage Preservation in WSNs", Elsevier, Ad Hoc Networks Journal, Vol. 7, No. 5, pp. 955-972, 2009.

[15] C. Song, M. Liu, J. Cao, Y. Zheng et, al , " Maximizing Network Lifetime Based on Transmission Range Adjustment in WSNs", Elsevier, Computer Communication Journal, Vol. 32, No. 11, pp. 1316-1325, July 2009.

[16] Xiaobing, G. Chen, S.K. Das, "Avoiding Energy Holes in WSNs with Non-Uniform node Distribution", IEEE Transactions on Parallel and Distributed System, Vol. 19, No. 5, pp. 710-720, 2008.

[17] O. Younis, S. Fahmy, "HEED: A Hybrid Energy Efficient Distributed Clustering Approach for Ad Hoc Sensor Networks", IEEE Transactions on Mobile Computing, Vol. 3, No. 4, pp, 366-379, October 2004.

[18] Y. Hu, N. Yu, X. Jia, "Energy Efficient Real-Time Data Aggregation Sensor Networks", In Proceedings of International Conference on Wireless Communications and Mobile Computing, Vancouver, British Columbia, Canada, pp. 803 – 808, 2006.

[19] Wang, G. Zhang, "DECP: A Distributed Election Clustering Protocol for Heterogeneous Wireless Sensor Network", In Proceedings of 7th International Conference on Computational Science (ICCS), Part III, LNCS, Beijing China, Vol. 489, pp. 105-108, 27-30 May 2007.

[20] W. Su, T.C. Bougioklis, "Data Fusion Algorithms in Cluster-Based WSNs Using Fuzzy Logic Theory", In Proceedings of 11th International Conference on Communications WSEAS, Agios Nikolaos, Crete Island, Greece, Vol. 11, pp. 291-299, 2007.

[21] H. Cam, S. Ozdemir, P. Nair, D. Muthuavinashiappan, "ESPDA: Energy-Efficient and Secure Pattern-based Data Aggregation for WSNs", In Proceedings of 2nd IEEE Conference on Sensors, Toronto, Canada, pp. 732-736, 22-24 October 2003.

[22] B. Zeng, J. Wei, T. Hu, "An Energy-Efficient Data Fusion Protocol for Wireless Sensor Network", In Proceedings of 10th International Conference on Information Fusion", pp. 1-7, 9-12 July 2007.

[23] C. Stefano, N. Chilamkurti, S. Zeadally, "A Novel Centralized Clustering Algorithm for Energy Efficient WSNs", International Journal of Autonomous and Adaptive Communications Systems, Vol. 1, No. 2, pp. 242 – 261, 2008.

[24] R. Guerraoui, A. Schiper, "Fault-Tolerance by Replication in Distributed Systems", In Proceedings of 1996 Ada-Europe International Conference on Reliable Software Technologies, 1088: 38–57, 1996.

[25] Devendra Prasad, R. B. Patel, Ajay Kr. Gautam "A Reconfigurable Group Aware Network Management (GANM) Protocol for WSNs", In proceeding of the IEEE International Conference on Advance Computing(IACC), Patiala, India, 6-7 March 2009.

[26] H.X. Ming, D. Jing, M. Jing, W. Zeyu, "Fault tolerant routing for wireless sensor grid networks", In Proceedings of IEEE Sensors Applications Symposium, pp. 66-70, 5 June 2006.

[27] A. Khadivi, M. Shiva, "FTPASC: A Fault Tolerant Power Aware Protocol with Static Clustering for WSNs", In Proceedings of IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, Montreal, Canada, pp.397-401, 19-21 June 2006.

[28] C. Intanagonwiwat, R. Govindan, D. Estrin, "Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks", In Proceeding of the 6th Annual ACM International Conference on Mobile Computing and Networking (MobiCom'00), Boston, MA, Aug. 2000.

[29] W. Heinzelman, A. Chandrakasan, H. Balakrishnan, "Energy-Efficient Communication Protocol for Wireless Microsensor Networks", In Proceeding of the 33rd Hawaii International Conference on System Sciences (HICSS'00), Jan. 2000.

[30] Y. Yu, D. Estrin, R. Govindan, "Geographical and Energy- Aware Routing: A Recursive Data Dissemination Protocol for Wireless Sensor Networks", UCLA Comp. Sci. Dept. Tech. Rep., UCLA-CSD TR-010023, May 2001.

[31] C. Karlof, D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", In Proceeding of the 1st IEEE International Workshop on Sensor Network Protocols and Applications (SNPA'03), May 2003.

[32] J. Newsome, E. Shi, D. Song, A. Perrig, "The Sybil Attack in Sensor Networks: Analysis and Defenses", In Proceeding of the 3rd IEEE International Symposium on Information Processing in Sensor Networks (IPSN'04), Berkeley, CA, Apr. 2004.

[33] M. Manzo, T. Roosta, S. Sastry, "Time Synchronization Attacks in Sensor Networks", In Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN'05), Alexandria, VA, Nov. 2005.

[34] S. Ganeriwal, S. Capkun, C. Han, M. B. Srivastava, “Secure Time Synchronization Service for Sensor Networks”, Proc. 4th ACM Wksp. Wireless Security (WiSe’05), Cologne, Germany, Sept. 2005.

[35] M. Zapata, N. Asokan, “Securing Ad Hoc Routing Protocols”, In Proceedings of the 3rd ACM Workkshop on Wireless Security (WiSe’02), Atlanta, GA, Sep. 2002.

[36] Y. Hu, D. Johnson, A. Perrig, “SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks,” In Fourth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA 02), Callicoon, NY, June 2002.

[37] P. Papadimitrators, Z. Haas, “Secure Link State Routing for Mobile Ad Hoc Networks”, In Proceedings of the IEEE Symposium Applications and the Internet Workshop, Jan. 2003.

[38] H. Yang, H Y. Luo, F Ye, S W. Lu, L Zhang, “Security in Mobile Ad Hoc Networks: Challenges and Solutions”, IEEE Wireless Communication, vol. 11, no. 1, pp. 38–47, Feb. 2004.

[39] Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, J. D. Tygar, “SPINS: Security Protocols for Sensor Networks”, Mobile Computing and Networking Rome, Italy, 2001.

[40] J. Deng, R. Han, S. Mishra, “A Performance Evaluation of Intrusion-Tolerant Routing in Wireless Sensor Networks”, In Proceedings of the 2nd IEEE International Workshop Information Processing in Sensor Networks (IPSN’03), Palo Alto, CA, Apr. 2003.

[41] R. D. Pietro et al., “LKHW: A Directed Diffusion-Based Secure Multicast Scheme for Wireless Sensor Networks”, In 32nd IEEE International Conference on Parallel Processing (ICPP 2003), Kaohsiung, Taiwan, 6-9 October 2003.